Department of Homeland Security Daily Open Source Infrastructure Report for 29 January 2009

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

- The San Francisco Chronicle reports that an oil tanker leaving the Port of San Francisco lost power on Tuesday just west of the Golden Gate Bridge and was escorted back into the bay for repairs, a U.S. Coast Guard spokesman said. (See item **2**)
- According to the Federal Aviation Administration Safety Team, on February 1, the International Cospas-Sarsat Organization (United States included) will terminate processing of distress signals emitted by 121.5 MHz Emergency Locator Transmitters. Currently, only 12-15 percent of the registered aircraft in the United States are flying with 406 MHz ELTs. (See item **13**)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − [http://www.esisac.com]

1. *January 27, Reuters* – (National) **U.S. ice storm power outages climb to 160,000.** A severe winter storm, with freezing rain that snapped trees and power lines, knocked out electricity to more than 161,000 customers in at least six states, U.S. utilities said on January 27. Parts of Arkansas and Kentucky were the hardest hit on January 27 as the winter storm moved southward. A band of icy rain stretched from northern Texas, across Oklahoma, Arkansas, Missouri, Kentucky and into West Virginia. Entergy Corp's Arkansas utility reported 54,000 outages while American Electric Power's SWEPCO

unit reported nearly 34,000 outages, mostly in Arkansas. In Kentucky, E.ON's utility reported 44,000 customers without power; AEP's Kentucky unit said outages climbed to 5,300 in the afternoon. By early evening, Oklahoma Gas & Electric had restored power to more than 5,000 customers, about half the number that lost service earlier in the day, while AEP's Tulsa-based Oklahoma utility saw only about 1,500 outages across its service territory. Dallas-based Oncor reported outages along the Texas-Oklahoma border as utility crews braced for icy rain and freezing temperatures to move into the Dallas-Fort Worth area overnight, possibly leaving thousands of customers without electricity.
Source:
http://www.reuters.com/article/rbssIndustryMaterialsUtilitiesNews/idUSN2748380820090128

2. *January 27, San Francisco Chronicle* – (California) **Tanker loses power, escorted into bay for repairs.** An oil tanker leaving the Port of San Francisco for Ecuador lost power January 27 just west of the Golden Gate Bridge and was escorted back into the bay for repairs, a U.S. Coast Guard spokesman said. The 741-foot Overseas Cleliamar had unloaded all of its oil at the Port of San Francisco and was carrying no cargo when it lost power at shortly after 5 p.m. The ship did not hit anything, and no pollution was believed to have been released, said a Coast Guard petty officer. The ship lost propulsion just after passing under the Golden Gate Bridge. The San Francisco ship pilot directed the ship to drop anchor near Point Diablo on the Marin side of the Golden Gate. The 32-member crew was able to restore power after about ten minutes. The Coast Guard received the call of distress at 5:22 p.m. A Coast Guard cutter and tugboats escorted the ship back into the bay for repair, although the ship was moving under its own power. He said Coast Guard helicopters flew over the scene and saw no signs of spilled oil or other pollution.
Source:
http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/01/28/BABI15IFVI.DTL

[Return to top]

Chemical Industry Sector

3. *January 28, Plainfield Star* – (Indiana) **City water well shut after fertilizer spill.** One of the wells providing water to Plainfield has been shut down as a precaution after a chemical fertilizer spill at a nearby business. Plainfield has several wells in other locations around the Hendricks County community, so the town has plenty of water from its other sources, according to the town engineer. The leak at Stanley Fertilizer Co. was detected on December 22, but information did not surface until January 26 at a Plainfield Town Council meeting. The council authorized spending up to $20,000 for a series of wells and testing to monitor the movement and quality of underground water around the municipal well in Franklin Park, to get an early warning before any contaminant can reach the city water source. Belcher said a pipe or valve on a large storage tank at the fertilizer plant became frozen and broke. Leaking liquid filled a shallow area around the tank intended to contain spilled liquids, and then it overflowed. The town will ask for repayment of its expenses from Stanley Fertilizer. How much

liquid fertilizer may have leaked is unclear.
Source:
http://www.indystar.com/article/20090128/LOCAL0505/901280346/1020/LOCAL05

4. *January 27, Kansas City Star* – (Kansas) **Chemical company official pleads guilty in illegal dumping.** The president of a St. Joseph chemical company pleaded guilty in federal court on January 27 to illegally dumping pesticide-contaminated wastewater into the city's sewer system for two years. He also entered guilty pleas on behalf of his company, HPI Products Inc., to an identical dumping charge and to illegally storing corrosive and toxic chemicals — such as chlordane, selenium and heptachlor — at the plant without the proper permits. HPI long has been the focus of state and federal enforcement efforts. Authorities have inspected and searched the business' numerous warehouses for three years, according to a civil lawsuit filed by the federal and state governments in December 2008. In that complaint, government lawyers alleged that HPI generated and improperly stored and disposed of hundreds of thousands of pounds of hazardous wastes for more than 20 years. According to the lawsuit, three HPI facilities, including one operating next to a day-care center, "pose an imminent and substantial risk of endangerment to health or the environment." The improper storage of chemicals at those facilities also posed the potential for fire and explosion, lawyers alleged.
Source: http://www.kansascity.com/news/local/story/1004706.html

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

5. *January 28, Reuters* – (Florida) **Progress shuts Fla. Crystal River 3 reactor.** Progress Energy Inc. shut Unit 3 at the Crystal River power station in Florida for short-term work on January 27, a spokeswoman for the plant said on January 28. She said workers were calibrating some equipment when some blown fuses caused a bus in the switchyard to trip, resulting in the loss of a feed water booster pump and a condensate pump. That led operators to manually shut the reactor from full power.
Source:
http://www.reuters.com/article/rbssIndustryMaterialsUtilitiesNews/idUSN2850908420090128

[Return to top]

Defense Industrial Base Sector

6. *January 28, Flight International* – (National) **Boeing spins quality line.** A seven-month streak of high-profile manufacturing breakdowns — with both criminal and accidental causes — have baffled the rotorcraft community. In early January, a disgruntled assembly worker was sentenced to five months in jail for intentionally damaging a CH-47 last May. Another act of suspected sabotage discovered at the same time has never been resolved. Boeing ordered a safety stand-down on the CH-47 line in October and halted work on the V-22 line in November to investigate serious mistakes. The Defense Contract Management Agency (DCMA) is investigating the discovery two weeks ago of

a socket wrench inside an MH-47G after it was delivered to Blue Grass Army Depot in Richmond, Kentucky. So far, the problems have not cost Boeing new business. In August, the U.S. Army signed a $4.3 billion, multi-year deal for 181 new CH-47Fs and MH-47Gs. To be sure, all manufacturers sometimes lose tools or deliver aircraft with small defects. But Boeing's vice president for rotorcraft acknowledges that the Philadelphia site's record over the last year is "a lot worse than we've ever seen." He acknowledged that new investments in the production line lagged after 2005, creating an atmosphere that allowed mistakes in quality to start rising. The sudden outbreak of errors late last year prompted the executive to call a Saturday morning meeting of 200 managers, who concluded that they were failing to follow quality control processes. Since that meeting, there have been "significant changes to process", he says. "All in all, what we've put in place now has satisfied DCMA that we have a better control over [foreign object debris] quality and tool control than we had last year."
Source: http://www.flightglobal.com/articles/2009/01/28/321580/boeing-spins-quality-line.html

[Return to top]

Banking and Finance Sector

7. *January 27, CNN* – (Florida) **Investment fund manager facing fraud charges surrenders.** A missing Florida fund manager, whose $300 million in investment funds are actually worth less than $1 million, according to a federal lawsuit, has turned himself in to face fraud charges, the Federal Bureau of Investigation said on January 27. The 76-year-old suspect, "recently transferred at least $1.25 million from two of the funds to secret bank accounts that he controlled," according to a filing last week in federal court by the Securities and Exchange Commission. The suit, filed January 21 in U.S. District Court in Tampa, charged the suspect with fraud "in connection with six hedge funds" in which he was principal investment adviser. Accompanied by two defense lawyers, the suspect turned himself in to the Tampa FBI field office and was taken into custody around 9:45 a.m. on January 27, a FBI spokesman said.
Source: http://www.cnn.com/2009/CRIME/01/27/fund.manager.surrender/index.html

8. *January 28, Seacoastonline.com* – (New Hampshire) **Service Credit Union advises members to avoid phone scam.** Service Credit Union is warning that telephone scammers are attempting to obtain personal information from ATM/Visa Check cardholders. Area residents, members and nonmembers, are receiving computer-generated calls claiming to be from Service Credit Union. The call claims account information was breached and directs the cardholder to press 1 to give his or her debit card information to reactivate any cards. Personal information requested includes account number, card expiration date and personal identification number. Service Credit Union does not solicit personal information over the phone, and if residents receive questionable calls, they should not provide any personal information, said the chief executive of Service Credit Union. If residents receive a suspicious call, they should notify Service Credit Union by e-mail and call the local authorities.
Source: http://www.seacoastonline.com/articles/20090128-NEWS-901280394

9. *January 28, Bloomberg* – (National) **FDIC may run 'bad bank' in plan to purge toxic assets.** The Federal Deposit Insurance Corp. (FDIC) may manage the so-called bad bank that the Presidential Administration is likely to set up as it tries to break the back of the credit crisis, two people familiar with the matter said. The FDIC chairman is pushing to run the operation, which would buy the toxic assets clogging banks' balance sheets, one of the two people said. The chairman is arguing that her agency has expertise and could help finance the effort by issuing bonds guaranteed by the FDIC, a second person said. The President's team may announce the outlines of its financial-rescue plan as early as next week, an administration official said. The bad-bank initiative may allow the government to rewrite some of the mortgages that underpin banks' bad debt, in the hopes of stemming a crisis that has stripped more than 1.3 million Americans of their homes. Some lenders may be taken over by regulators and some management teams could be ousted as the government seeks to provide a shield to taxpayers.
   Source: http://www.bloomberg.com/apps/news?pid=20601087&sid=avQ3LP7o44oU&refer=home

[Return to top]

Transportation Sector

10. *January 28, WJLA 7 Washington* – (Maryland) **Red Line delays due to smoke reports at Metro station.** Red line riders on Metrorail the morning of January 28 should be prepared for delays. Smoke has been reported on the tracks at the Bethesda station and track workers are investigating. Near Bethesda, a track malfunction is delaying the red line: trains are sharing a track between Friendship Heights and Medical Center. The Bethesda station has reopened.
    Source: http://www.wjla.com/news/stories/0109/589542.html?ref=rs

11. *January 28, KCRA 3 Sacramento* – (California) **2 escape injury in emergency plane landing.** A small plane was forced to make an emergency landing Tuesday in a field near Turlock Reservoir after the aircraft's engine blew a rod and failed, police said. An instructor taking a student for a flight managed to set the plane down safely near Davis Road between Hickman and the reservoir, a deputy said. Authorities said the pilot and the student were not injured. The pilot said he followed protocol by shutting off the plane's fuel prior to landing.
    Source: http://www.msnbc.msn.com/id/28877680/

12. *January 27, WTOP 103.5 Washington, D.C.* – (Maryland) **Purple line pick.** The Montgomery County Council unanimously approved a light rail option on January 27 as the preferred alternative for the planned Purple Line in Maryland. The decision will now go to state transportation leaders for the final say. On WTOP's Ask the Governor Program last week, the Maryland governor all but confirmed light rail will be the choice of the state, saying that option is the most feasible.
    Source: http://www.wtop.com/?sid=1585589&nid=689

13. *January 26, Federal Aviation Administration Safety Team* – (National) **406-MHz ELT**

requirement starts next month. On February 1, 2009, the International Cospas-Sarsat Organization (United States included) will terminate processing of distress signals emitted by 121.5 MHz Emergency Locator Transmitters (ELTs). Pilots flying aircraft equipped with 121.5 MHz ELTs after that date will have to depend on pilots of over flying aircraft and or ground stations monitoring 121.5 to hear and report distress alert signals, transmitted from a possible crash site. Currently only 12-15 percent of the registered aircraft in the United States are flying with 406 MHz ELTs. This means that there is at least an 85 percent chance that an aircraft in an accident will only transmit a 121.5 MHz signal, thus remaining silent to the satellites. It will be up to other pilots monitoring the 121.5 MHz frequency in the cockpit to alert Search and Rescue authorities to accidents involving 121.5. If a 121.5 MHz ELT is heard on guard, pilots must report to the nearest air traffic control tower or Flight Service Station, the time and location of when you first detect the ELT, when it is the loudest, and when it drops off your radio. Cospas-Sarsat System has been and will continue processing emergency signals transmitted by 406 MHz ELTs. These 5 Watt digital beacons transmit a much stronger signal, are more accurate, verifiable and traceable to the registered beacon owner.
Source: http://www.amtonline.com/article/article.jsp?siteSection=1&id=7260

[Return to top]

Postal and Shipping Sector

14. *January 27, Associated Press* – (Missouri) **Federal court in KC receives suspicious envelope.** Authorities are investigating after a suspicious envelope arrived Tuesday at the U.S. District Court in Kansas City. Employees reported to authorities that the envelope was leaking a yellowish-green powdery substance. The FBI says the envelope was mailed from a Jefferson City prison and addressed to the chief clerk. A hazardous materials crew was dispatched to the courthouse. Preliminary tests results revealed that the substance was not hazardous. No one was injured, and the building was not evacuated. The FBI and U.S. Postal Service are investigating.
Source: http://www.nebraska.tv/Global/story.asp?S=9744154&nav=menu605_1

[Return to top]

Agriculture and Food Sector

15. *January 26, ScienceDaily* – (Iowa; Illinois) **MRSA found in Midwestern swine, workers.** The first study documenting methicillin-resistant Staphylococcus aureus (MRSA) in swine and swine workers in the United States has been published by University of Iowa researchers. The investigators found a strain of MRSA, known as ST398, in a swine production system in the Midwest, according to the new study. “Our results show that colonization of swine by MRSA was very common in one of two corporate swine production systems we studied,” said an associate professor of epidemiology in the University of Iowa College of Public Health and lead author of the study. “Because ST398 was found in both animals and humans, it suggests transmission between the two. Our findings also suggest that once MRSA is introduced, it may spread

broadly among both swine and their caretakers. Agricultural animals could become an important reservoir for this bacterium," she added. The University of Iowa study was the first to investigate carriage of MRSA among swine and swine farmers in the United States. For the study, investigators analyzed nasal swabs of 299 swine and 20 swine workers from two different production systems in Iowa and Illinois. The investigators recommended that future studies assess the risk of MRSA disease among swine workers and their contacts, survey retail meat products for MRSA contamination, study larger populations of swine and humans to define the epidemiology of MRSA within swine operations, and assess MRSA carriage rates in other livestock.
Source: http://www.sciencedaily.com/releases/2009/01/090122202804.htm

[Return to top]

Water Sector

16. *January 28, Associated Press* – (District of Columbia) **Lawmakers seek probe of lead crisis in D.C.** Council of the District of Columbia members want an investigation of whether public health and water utility officials misled the public on the health effects of record-breaking lead levels in city drinking water between 2001 and 2004. Council members wrote to the District of Columbia inspector general Tuesday, asking for an investigation of whether authorities "negligently or intentionally" misled the public. The inquiry follows a health study that found about 42,000 children were put at high risk because of the elevated lead levels. The study from Virginia Tech and Children's National Medical Center contradicts statements from federal and local authorities that said the lead crisis had not affected residents' health. Lead concentrations began rising drastically in 2001 — and remained high for three years — after a new chemical was used to treat the water.
Source: http://www.examiner.com/a-1819495~Lawmakers_seek_probe_of_lead_crisis_in_DC.html

[Return to top]

Public Health and Healthcare Sector

17. *January 28, Palm Springs Desert Sun* – (California) **Desert Regional nurse tests positive for tuberculosis.** A nurse who worked in Desert Regional Medical Center intensive care unit for newborns has tested positive for tuberculosis, hospital officials said Tuesday. The Center sent letters to parents of 124 babies who may have been exposed to the nurse during a three-month window, said the hospital's chief medical officer. The Riverside County Department of Public Health is asking the parents to bring the babies in for testing. The nurse, who was diagnosed about three weeks ago, is in home isolation and is being treated, hospital officials said. All hospital workers who deal directly with patients are tested every six months.
Source: http://www.mydesert.com/article/20090128/NEWS01/901280324/-1/newsfront

18. *January 27, Health Day News* – (National) **'Wired' hospitals post lower death, complication rates.** The more "wired" a hospital is, the lower its rate of patient deaths

and complications, a new study finds. Automating hospital information systems also saves centers money, the researchers report. Although there are many kinks to be worked out, said a senior fellow at the National Center for Policy Analysis in Dallas, "I assume that over the course of the next few years, with or without the government's prodding, that we will begin to integrate this more and more, because it is a good idea, but I think there will be some growing pains about which system and how and whether it talks to neighboring hospitals and so on." The authors compared inpatient death rates, complications, length-of-stay, and cost associated with greater and lesser levels of automation in 41 Texas hospitals.
Source: http://www.healthday.com/Article.asp?AID=623470

19. *January 27, University of Pennsylvania* – (Pennsylvania) **Penn study identifies how Ebola virus avoids the immune system.** Researchers at the University of Pennsylvania School of Medicine have likely found one reason why the Ebola virus is such a powerful, deadly, and effective virus. Using a cell culture model for Ebola virus infection, they have discovered that the virus disables a cellular protein called tetherin that normally can block the spread of virus from cell to cell. These findings appear online this week in the Proceedings of the National Academy of Sciences. "This information gives us a new way to study how tetherin works," says the study author, an associate professor of Microbiology at the University of Pennsylvania School of Medicine. Previous research had found that tetherin plays a role in the immune system's response to HIV-1, a retrovirus, and that tetherin is also disabled by HIV. These new studies reveal that human cells also use this defense against other types of viruses, such as Ebola, that are not closely related to HIV-1. "Because we see such broad classes of viruses that are affected by tetherin, it's possible that all enveloped viruses are targets of this antiviral system," he says. "If so, then understanding how tetherin works and how viruses escape from the effect of tetherin will be very important."
Source: http://www.uphs.upenn.edu/news/News_Releases/2009/01/tetherin-ebola.html

[Return to top]

Government Facilities Sector

20. *January 28, Reuters* – (National) **U.S. retrieves MP3 player with military files.** A New Zealand man who bought a second-hand MP3 player that contained U.S. military files on personnel who served in Afghanistan and Iraq handed it over to U.S. officials on Wednesday, New Zealand media reported. The 29-year old man bought the $10 MP3 at a thrift shop in Oklahoma, but when he plugged it in discovered it contained 60 U.S. military files, said New Zealand television program One News, which broke the story. U.S. embassy officials in New Zealand spoke to the New Zealand man on Tuesday night and swapped his old MP3 player for a new one on Wednesday, New Zealand Press Association said. The man said the officials asked him what computers the player's files had been loaded onto and whether he had made copies and then photographed some of the files, but would not say how sensitive the information was.
Source: http://in.reuters.com/article/worldNews/idINIndia-37700520090128
See also: http://www.abc.net.au/news/stories/2009/01/28/2476801.htm?section=world

21. *January 27, Associated Press* – (Idaho) **Idaho man exposed to radiation.** Officials at Idaho National Laboratory say an employee cleaning up radioactive waste has been exposed to a low dose of radiation. Investigators are blaming an equipment malfunction for causing the exposure, which occurred January 30 in an area contaminated by 50 years of nuclear weapons testing. They say a worker assigned to the Idaho Cleanup Project was working with americium, the substance used in household smoke detectors. It is used to calibrate tools designed to detect radioactivity in its cleanup efforts. A spokesman for the Idaho National Laboratory says the worker discovered the contamination while self-monitoring before exiting the facility. The employee was not harmed and has returned to work.
Source: http://seattlepi.nwsource.com/local/6420ap_id_radiation_worker.html

22. *January 26, Packer* – (Florida) **New USDA lab planned for South Miami.** A new laboratory for research and development of commodity treatments and port inspection technologies should open in South Miami, Florida, by the end of 2009. The U.S. Department of Agriculture's Animal and Plant Health Inspection Service plans to open the new laboratory because of its proximity to both sea and air ports. The facility will be called Agriculture Quarantine and Inspection and Port Technology Methods Development Laboratory, reflecting its purpose to find better ways to protect the country's agricultural and natural resources from foreign plant pests and diseases, according to a news release.
Source: http://www.thepacker.com/icms/_dtaa2/content/wrapper.asp?alink=2009-14544-55.asp&stype=topnews&fb

[Return to top]

Emergency Services Sector

23. *January 28, United Press International* – (National) **Radiation protective fabric patented.** Florida-based Radiation Shield Technologies announced its new radiation protective fabric has received a patent from the U.S. Patent and Trademark Office. Radiation Shield Technologies says its Demron fabric, developed to offer protections from chemical, biological, and radiological threats, received the patent. Officials say the nanotechnology developed for the Demron fabric was the key advancement that led to the patent. Radiation Shield Technologies says Demron is a lightweight nuclear-radiation blocking garment that can be crafted into full-body suits, vests, and blankets, among other applications for the defense and homeland security markets.
Source:
http://www.upi.com/Security_Industry/2009/01/28/Radiation_protective_fabric_patented/UPI-40741233158859/

24. *January 27, Federal Computer Week* – (National) **FEMA seeks IT for ID management.** The Federal Emergency Management Agency (FEMA) wants innovative pricing options for software that would control access and identity management of the agency's computer systems to deal with surges in use. FEMA published a Request for Information on January 23 seeking to identify existing commercial-off-the-shelf or government-based solutions that would meet its needs. Responses are due by February

6. The solution must accommodate requirements for a variety of users, including FEMA personnel, contractors, state and local partners, first responders, disaster victims, and Federal Government partners, the agency said. "It is a desire of the agency to obtain a pricing approach that supports the variable nature of the size of the FEMA user community," the notice states. "During periods after large disasters and other events, the agency user base may substantially increase in size for a period of time. The vendors should provide creative pricing structures where possible such that FEMA does not have to pay [or pay less] for accounts that are infrequently used, but still active." The proposed new solution must recognize and manage spheres and levels of access for each user, and sometimes recognize multiple privileges for a single user, depending on the assignments, the notice said.
Source: http://fcw.com/articles/2009/01/27/fema-seeks-it.aspx

[Return to top]

Information Technology

25. *January 27, PC World* – (International) **Security firm sees alarming rise in 'transient' threats.** Anti-virus firm AVG Technologies says an alarming rise in the number of virus-laden sites that are here today and gone tomorrow is causing security experts to re-think traditional virus protection strategies. AVG reports the number of Web sites set up to steal one's data has nearly doubled from about 150,000 per day to 300,000 since October 2008. More alarming to AVG is the fact those sites are short lived and vanish sometimes within 24 hours. These "transient threats" make maintaining lists of dangerous Web sites extremely hard to manage, said the chief research officer for AVG. "Security firms can no longer rely on just blacklisting sites," the chief research officer said. AVG, like many other anti-virus companies, keeps track of rogue sites and updates its desktop anti-virus software with that list. But as the churn of new threats increases at an alarming rate blacklist databases become increasingly less effective.
Source:
http://www.pcworld.com/article/158401/security_firm_sees_alarming_rise_in_transient_threats.html

26. *January 27, TechCrunch.com* – (International) **Report: click fraud at record high.** 17.1 percent of all clickthroughs on Web advertising are the result of clickfraud, the act of clicking on a Web ad to artificially increase its click-through rate, according to the latest report from Click Forensics, a company that specializes in monitoring and preventing Internet crime. The level of clickfraud is the highest the company has seen since it started monitoring for it in 2006, dashing hopes that it might hold steady in 2008. The company recorded a rate of 16.3 percent in the first fiscal quarter of 2008 (Q1). Also alarming is the fact that over 30 percent of click fraud is now coming from automated bots — a 14 percent increase from last quarter and the highest rate Click Forensics has seen since it started collecting data. Click fraud for ads on content networks like Google AdSense and Yahoo Publisher Network was up to 28.2 percent from 27.1 percent last quarter, though that figure has decreased since Q4 2007, when it was at 28.3 percent. Outside of the United States, Click Forensics reports that the most click fraud came from Canada (which contributed 7.4 percent), Germany (3 percent),

and China (2.3 percent). Click Forensics also notes that it has seen a reemergence with some old-hat tricks, like link farms. The company speculates that the increase may be tied to the poor economy, which has spurred a rise in activity like phishing and other cybercrime.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2009/01/28/AR2009012800046.html

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: http://www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Communications Sector

27. *January 28, Heise Media* – (International) **Windows mobile Bluetooth vulnerability allows access to any files.** A directory traversing vulnerability in the Bluetooth OBEX-FTP server of Windows Mobile 6 allows attackers to access files outside of the permitted list. According to the report, using "../" or "..\\" as part of the path name, is sufficient to traverse to other directories. An attacker could use the technique to copy files from a device, or to install their own software, such as a key logger, or other spyware. The issue does require that the targeted hand held device is paired with the attacking device, which is usually only possible with the owner's consent. There are, though, situations where a user may wish to restrict access to their files for paired devices, and the problem means that these restrictions are only partially effective. The discoverer of the bug has published a detailed guide to the problem.
Source: http://www.heise-online.co.uk/security/Windows-Mobile-Bluetooth-vulnerability-allows-access-to-any-files--/news/112510

28. *January 28, Associated Press* – (Arkansas; Kansas) **Cox to test new way to handle Internet congestion.** Cox Communications, the third-largest U.S. cable company, stepped on to the battleground of the "Net Neutrality" issue on January 27, saying it will be trying out a new way to keep its subscribers' Internet traffic from jamming up. Starting on February 9 in parts of Kansas and Arkansas, Cox will give priority to Internet traffic it judges to be time-sensitive, like Web pages, streaming video, and online games. File downloads, software updates, and other non-time sensitive data may be slowed if there is congestion on the local network, Cox said. The news is sure to revive the debate about Net Neutrality, or the question of how much Internet service providers like Cox can interfere with subscriber traffic.
Source: http://tech.yahoo.com/news/ap/20090128/ap_on_hi_te/tec_cox_internet

29. *January 26, CNET News* – (National) **Congressman wants to ban silent camera phones.** Earlier in January, a U.S. Representative from New York introduced a bill in the U.S. House of Representatives that would ban camera phones from having a silent

mode when taking a picture. The Camera Phone Predator Alert Act (H.R. 414) would "require any mobile phone containing a digital camera to sound a tone whenever a photograph is taken." What is more, the bill would prohibit such handsets from being equipped with a means of disabling or silencing the tone. Enforcement would be through the Consumer Product Safety Commission. The text of the bill is short, and the Representative's office has not released any public statements. At the time of this writing, the bill has been referred to the House Energy and Commerce. The Camera Phone Predator Alert Act has no co-sponsors.
Source: http://news.cnet.com/8301-17938_105-10150671-1.html?part=rss&tag=feed&subj=News-Wireless

[Return to top]

Commercial Facilities Sector

30. *January 28, Atlanta Georgia Constitution* – (Georgia) **Atlanta man arrested on bomb threat charges.** Authorities have arrested an Atlanta man on charges of making a series of bomb threats against the Atlanta Housing Authority over four days. An FBI spokesman says the 46-year-old was taken into custody on January 27 by the agency's Joint Terrorism Task Force. The FBI says the man is accused of making several telephone bomb threats between Monday and Thursday of last week. On January 22, the Housing Authority office was shut down for about three hours while authorities searched the building. No bomb was found.
Source: http://www.fortmilltimes.com/124/story/438276.html

31. *January 27, Associated Press* – (Iowa) **Michigan man charged with threatening call in Iowa.** A man who authorities say made a threatening phone call to a Red Robin restaurant in Cedar Rapids, Iowa has been arrested by police in Ohio. The 48-year-old man of Wyoming, Michigan is charged with making death threats and disruption of interstate commerce. Police say the call the man made to the Cedar Rapids restaurant on December 30 caused it to be closed for about an hour while officers checked the building and surrounding area. He is accused of telling an employee that he was in the parking lot and would shoot everyone inside. The man also allegedly placed as many as 60 threatening calls to tanning salons and restaurants in 10 states, warning female employees that he had a gun trained on them. The suspect is in custody in Ohio.
Source: http://www.kcrg.com/news/local/38478869.html
See also: http://www.kwwl.com/Global/story.asp?S=9741254&nav=menu82_2_1

[Return to top]

National Monuments & Icons Sector

32. *January 28, Washington Post* – (Arizona) **Interior ignored science when limiting water to Grand Canyon.** Interior Department officials ignored key scientific findings when they limited water flows in the Grand Canyon to optimize generation of electric power there, risking damage to the ecology of the national landmark, according to documents obtained by the Washington Post from the group Public Employees for

Environmental Responsibility. A January 15 memo written by the Grand Canyon National Park superintendent suggests that the department produced a flawed environmental assessment to defend its actions against environmentalists in court. The Grand Canyon Trust, an advocacy group, has sued the Department of Interior for reducing the flow of water from Glen Canyon Dam at night, when consumer demand for electricity is low, on the grounds that the policy hurts imperiled fish species and erodes the canyon's beaches. The Federal Government has spent about $100 million studying water flows on the Colorado River which indicate that the ecosystem would benefit from occasional short bursts of massive amounts of water along with more regular flows during the day and night. A Bureau of Reclamation spokesman said he could not discuss the controversy in detail because it was "under litigation," but he noted that a federal judge had already ruled that Interior had not violated any laws in drafting its operating plan for the Colorado River.
Source:
http://www.washingtonpost.com/wp-dyn/content/article/2009/01/27/AR2009012703283.html

[Return to top]

Dams Sector

33. *January 28, Reno Gazette-Journal* – (Nevada) **Truckee levee work begins east of U.S. 395.** Construction of the first levee and flood wall associated with a major flood-control project on the Truckee River has started in Reno. Heavy equipment began moving dirt on January 26 just east of U.S. 395. River restoration associated with the flood project started at two locations on the lower Truckee River late last year, but this project is the first actual construction designed to help control flooding in the Reno-Sparks area. As such, the $5.8 million levee and flood wall represents a cornerstone of sorts for the overall flood project, expected to cost between $1.2 billion and $1.6 billion. The earthen levee and concrete floodwall will stretch about 2,300 feet along the south bank of the Truckee River between U.S. 395 and the Glendale Avenue Bridge.
Source: http://www.rgj.com/article/20090128/NEWS04/901280433/1321/NEWS

34. *January 28, Chico Enterprise Record* – (California) **Supervisors won't sign pact to assume legal liability for levees.** In Butte County, California, a hearing about taking on legal liability for area levees ended on January 27 the way it began, with everybody involved saying no. On January 27, the Butte County Board of Supervisors heard its second presentation about a Federal Emergency Management Agency (FEMA) plan to redraw flood hazard maps in the county. What makes this re-mapping significant is the way FEMA is treating existing levees. In the past if a levee met the required physical dimensions to handle a so-called "100-year flood," the feds accepted it as adequate. This time, according to the land development division manager for the county Department of Public Works, FEMA is demanding "certification" the levee is high enough, holds the necessary amount of water, is properly maintained, and is built on soil that would stand the rigors of the 100-year flood. Under FEMA's rules, any levee that is not officially certified as meeting the standard will be treated in the flood mapping as if it does not exist.

Source: http://www.chicoer.com/news/ci_11569329

35. *January 27, Lawrence Journal-World* – (Kansas) **Sedimentation threatens sources of drinking water, flood control.** State officials are warning that Kansas reservoirs and lakes are quickly filling with sediment, which could lead to severe water shortages. At stake is a $6 billion investment in the reservoirs that provide drinking water to two-thirds of Kansans. In addition, the reservoirs are used for flood control and recreation. The highest areas of sedimentation are in eastern Kansas. Since 1974, Lake Perry has lost 18 percent of its capacity to 92 million cubic yards of sediment. Six lakes have lost more than 20 percent of their capacity, including Fall River, Tuttle Creek, Kanopolis, Toronto and John Redmond Reservoir, which has lost approximately 45 percent of its capacity. The culprit is runoff and bank erosion. "Many of our reservoirs are silting in much faster than anticipated, than their designed life," said a state biologist and director of the Kansas Biological Survey. A spokesman for the Kansas Department of Health and Environment Bureau of Environmental Field Services said there are things that can be done to address the problem, such as dredging, building secondary dams, and constructing new reservoirs.
Source: http://www2.ljworld.com/news/2009/jan/27/sedimentation-threatens-sources-drinking-water-flo/

36. *January 27, Reuters* – (National) **U.S. stimulus may bypass locks, dams — corn growers.** The creaky system of locks and dams on the Mississippi River that moves $300 billion of goods through the inland United States each year may not be eligible for much funding from the U.S. stimulus plan, the head of the National Corn Growers Association said January 27. The U.S. Army Corps of Engineers (USACE) has done the engineering work to expand the waterway's capacity, but Congress has not yet appropriated funding for the overhaul, he said. The entire locks and dams project would take about 15 years and $2.2 billion to complete, said the director of public policy for the corn growers. But the USACE could make significant progress on one or two of the locks in the next two years with an infusion of $1 billion to $1.5 billion, he said. The old locks cause bottlenecks, limiting barge shipments down the Mississippi, which handles about 60 percent of U.S. grain exports worth about $8.5 billion. Petroleum, chemicals, and other bulk goods also move on the system.
Source: http://www.forbes.com/feeds/reuters/2009/01/27/2009-01-28T002427Z_01_N27464839_RTRIDST_0_USA-STIMULUS-LOCKS-CORRECTED.html

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.
To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer